COUNTY OF SAN LUIS OBISPO

Countywide Information Security Program

Administrative Policy

Title: Information Security Program Acceptable Use Policy

Effective Date: April 2, 2004
Prepared by: Countywide Information Security Committee
Review Date: June 1, 2008
Approved by: Information Technology Executive Steering Committee
Approval Date: June 1, 2007

1. PURPOSE

The purpose of this policy is to outline the acceptable use of County Computing Assets (see DEFINITIONS).

2. SCOPE

This policy applies to all Users of County Computing Assets. Inappropriate use exposes the County to risks and threats to telecommunications, information systems, networks, facilities, and legal issues.

3. POLICIES

3.1. Overview

3.1.1. The County is committed to protecting itself from illegal or damaging actions, whether by intentional or unintentional means.

3.1.2. County Computing Assets are provided for conducting County business.

3.1.3. Effective security is a team effort involving the participation and support of every User of County Computing Assets. Every User must know this policy and conduct their activities in compliance with it.

3.1.4. A full listing of County Information Security Program Policies is listed under RELATED DOCUMENTS/POLICIES.

3.2. General Use and Ownership

3.2.1. The County may conduct audits or investigations on its Computing Assets to ensure compliance with this policy.

3.2.2. Nothing in this section will change the legal status of confidential or privileged information.

3.2.3. Users should be aware that the data they create on County Computing Assets is the property of the County, unless the legal ownership is otherwise defined by law, as in confidential or privileged information.

3.2.4. All Users acknowledge that there is no personal right of privacy for the User using County Computing Assets. The use of a password does not create a right to privacy.

3.2.5. Authorized individuals within the County may monitor equipment, systems, and network traffic at any time for security, network maintenance and policy compliance purposes (see EXCEPTIONS).

3.3. Electronic Mail

3.3.1. County provided Internet E-mail sent to, or received from an Internet address, if undeliverable for a variety of reasons, may have its contents reviewed for the sole purpose of determining addressability.

3.3.2. County provided virus protection will be maintained for all inbound and outbound E-mail. If possible, when an infected message is detected at the mail server, the virus protection software will attempt to clean it; if unable, it may delete the infected attachment or the entire message if needed to remove the virus. When an infected message is detected, a notification will be sent to the recipient and the E-mail administrator, regardless of whether the message is cleaned or deleted.

3.3.3. Message backup occurs by duplicating all messages and creating a storage copy. This procedure is performed nightly and held for a period of time. When authorized, messages can be restored from a backup copy. These procedures are intended for disaster recovery purposes, and not for customer convenience.

3.3.4. When establishing an E-mail ‘out of office’ agent, it is recommended that you do not automatically reply to E-mail from the Internet.

3.4. Use of County Provided E-mail and Internet for Personal Use

3.4.1. The County provides Internet services, E-mail services, telephone services, and computers to enable Users to conduct the County’s business in an efficient manner. These services and hardware systems are to be used in the direct conduct of the County’s business.

3.4.2. Users may occasionally use County provided Internet services, E-mail services, telephone services, and computers for personal use. The User must limit their use so that the County’s equipment is available for County use. The standard will be the same “reasonable use” standard that exists for use of County telephone equipment.

3.5. Security and Proprietary Information

3.5.1. Information contained on Internet/Intranet/Extranet-related systems is either confidential or public, as defined by organizational confidentiality guidelines. Examples of confidential information include, but are not limited to: medical information, personnel information, User data, vendor and bidder sensitive information, specifications, and other data. Users should take all necessary steps to prevent unauthorized access to this information.

3.5.2. All County Users must acknowledge having received the County’s Acceptable Use Policy (ATTACHMENT) annually, and are assigned accounts for their specific use based on their defined needs. Passwords are required to enable Users to keep their County Computing Assets secure. Users:

3.5.2.1.1. Are responsible for the security of their accounts.

3.5.2.1.2. Are not authorized to share their passwords.

3.5.2.1.3. Must change their password in accordance with individual application requirements.

3.5.3. Recommended Security Technologies

3.5.3.1. Password-protected screensavers, with automatic activation set at 10 minutes or less (of inactivity), are recommended on all PCs, laptops, and workstations.

3.5.3.2. Personal Digital Assistants (PDA) or other very portable digital equipment should power down and/or automatically be secured at 5 minutes or less when inactive.

3.5.3.3. It is recommended that Users log off the network when their workstations will be unattended for extended periods of time. All devices must require password re-authorization when re-activating.

3.5.3.4. Use encryption, when/where available, for information that Users consider sensitive or vulnerable in compliance with established departmental standards.

3.5.4. Because information contained on portable computers is especially vulnerable, exercise special care in the handling, storage and transportation of this equipment.

3.5.5. All computers that are connected to the County Internet/Intranet/Extranet, whether owned by the User or County, must continually execute approved virus-scanning software with a current virus database.

3.5.6. Do not open E-mail attachments from an unknown sender, as it may contain malicious software, generally known as Malware (see DEFINITIONS).

3.6. Unacceptable Use

3.6.1. The following activities are prohibited. The three lists below are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

3.6.1.1. System Activities

3.6.1.1.1. Any purpose which violates applicable U.S., state, local laws, or County policies and their implementing regulations.

3.6.1.1.1.1. Using a County Computing Asset to knowingly engage in viewing, reading, creating, conveying, downloading, transferring, transmitting, scanning, or printing:

3.6.1.1.1.1.1. Any Harmful Matter or Obscene Matter as those terms are defined in California Penal Code sections 311 and 313, which can be found on the State of California, Office of Legislative Counsel's Website;

http://www.leginfo.ca.gov/calaw.html

3.6.1.1.1.1.2. Any Matter in a manner that violates the San Luis Obispo County Policy Against Discriminatory Harassment;

3.6.1.1.1.1.3. Any illegal Matter (including child pornography) or sexually explicit images deemed by community standards to be obscene.

3.6.1.1.1.2. This provision does not apply to law enforcement and/or other County employees in situations where they are engaging in such activities in the performance of their job duties.

3.6.1.1.2. Using products that are not appropriately licensed for use by the County or those that violate the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software.

3.6.1.1.3. Abuse, damage, or exploitation of County Computing Assets.

3.6.1.1.4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the County or the User does not have an active license.

3.6.1.1.5. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws is illegal. Consult the appropriate management prior to exporting any material of this nature.

3.6.1.1.6. Exporting, exploiting, sharing, or using for personal gain, data contained within County Computing Assets; with a private enterprise, the public, or other Users without permission of the data owning department. This includes Users developing applications or accessing data for their own department, or another County department.

3.6.1.1.7. Knowingly introducing Malware programs into any County Computing Asset.

3.6.1.1.8. Engaging in fraudulent offers of products, items, or services originating from any County Computing Asset.

3.6.1.2. Network Activities

3.6.1.2.1. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access. For purposes of this section, “disruption” includes, but is not limited to, Network Sniffing, Pinged Floods, packet Spoofing (see DEFINITIONS), denial of service, and forged routing information for unauthorized purposes.

3.6.1.2.2. Executing any form of network monitoring that will intercept data not intended for the User’s workstation, such as port scanning or security scanning, is expressly prohibited.

3.6.1.2.3. Circumventing or mimicking (Spoofing) User authentication or security of any host, network, or account.

3.6.1.2.4. Interfering with or denying service to any Computing Asset other than the User’s own workstation (e.g., denial of service attack).

3.6.1.2.5. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable any Computing Asset, via any means, locally or via the Internet/Intranet/Extranet.

3.6.1.2.6. Providing information about, or lists of, County Users to parties outside the County, for other than authorized County business purposes.

3.6.1.2.7. Adding any networked component that is connected either directly to the County's Wide-Area-Network, or indirectly connected via a Local-Area-Network segment that creates the potential for a breach of the County's network.

3.6.1.3. E-mail and Communications Activities

3.6.1.3.1. Sending unsolicited E-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (i.e. E-mail spam).

3.6.1.3.2. Any form of harassment or discrimination via E-mail, telephone, or paging, whether through language, frequency, or size of messages.

3.6.1.3.3. Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type, pornography or fraudulent E-mail as listed on the Federal Trade Commission's Website:

http://www.ftc.gov/ftc/consumer/media_consumeralerts.shtm

3.6.1.3.4. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups, effectively producing newsgroup spam.

4. DEFINITIONS

4.1. COMPUTING ASSETS

Information of any kind processed by any means using County information processing systems, networks, software, equipment, materials, or implements which are owned, managed, operated, maintained, or in the custody or proprietorship of the County or private entities. This includes, but is not limited to, Internet, Intranet, and Extranet applications, operating systems, network operating systems, storage media, network accounts, E-mail, file transfer protocol, and documentation.

4.2. USER

Any end User of County Computing Assets including; elected officials, full-time, part-time, and temporary County officers, agents, employees, contractors, consultants, volunteers or any individual authorized to use County Computing Assets.

4.3. MALWARE

For "malicious software", is programming or files that are developed for the purpose of doing harm. Thus, Malware includes computer viruses, pervasive worms, Trojan horses, and E-mail bombs, etc.

4.4. MATTER

As defined in California Penal Code section 311 and 313, which can be found on the State of California, Office of Legislative Counsel's Website: http://www.leginfo.ca.gov/calaw.html

4.5. NETWORK SNIFFING

Hardware and software normally used for monitoring and troubleshooting problems on the network. Used illegally, this technology would improperly obtain data, or slow the network response time.

4.6. PINGED FLOODS

Pinging is diagnostically used to ensure that a host computer, which you are trying to reach, actually operates. Used illegally, the Ping program would tie up the network by constantly Pinging a workstation or server.

4.7. PONZI SCHEME

Named after scam artist Charles Ponzi, who was famous for offering to 'double your money in 90 days', early in the 20th century.

4.8. SPAM

Spam is unsolicited E-mail on the Internet, generally equivalent to unsolicited phone marketing calls, except that the User pays for part of the message since everyone shares the cost of maintaining the Internet.

4.9. SPOOF

To deceive for the purpose of gaining access to someone else's resources. For example, to fake an Internet address so that one looks like a certain kind of Internet user.

4.10. USENET NEWSGROUP

Usenet is a collection of User-submitted notes or messages on various subjects that are posted to servers on a worldwide network. Each subject collection of posted notes is known as a newsgroup.

5. **OTHER AGENCY INVOLVEMENT**

The Information Technology Department will work cooperatively with all County departments, outside governmental agencies, and vendors performing information technology work with the County, to ensure compliance with this policy.

6. EXCEPTIONS

6.1. County electronic mail (E-mail) records may be accessed with written permission to the County Chief Information Officer from the County Administrative Officer, or the User's department head.

6.2. A listing of Internet or Intranet sites visited by a User from a County Computing Asset may be requested with written permission to the County Chief Information Officer from the County Administrative Officer, or the User's department head.

6.3. In response to subpoenas.

6.4. In response to Freedom of Information Act or California Public Records Act requests, only County information normally available to the public may be accessed.

6.5. Interdepartmental records requests must be approved in writing by the County Administrative Officer prior to submission to the County Chief Information Officer.

6.6. Other access after consultation for legal review by County Counsel.

7. FORMS

ATTACHMENT: Acceptable Use Policy Acknowledgement, which is signed annually by each authorized User of County Computing Assets.

8. RELATED DOCUMENTS/POLICIES

8.1. San Luis Obispo County Policy Against Discriminatory Harassment
8.2. San Luis Obispo County Telephone Policy
8.3. State of Calilfornia Penal Code Sections 311, et seq. and 313, et seq.
8.4. Federal Trade Commission's Website of Fradulent E-mail
8.5. Information Security Program Policies in effect:
8.5.1. Acceptable Use Policy
8.5.2. Awareness, Training and Education Policy
8.5.3. Computer Forensics Policy
8.5.4. Incident Response Policy
8.5.5. IT Business Continuity Policy and Framework
8.5.6. IT Workforce Security Policy
8.5.7. Master Security Policy
8.5.8. Password and Authentication Policy
8.5.9. Patch Management Policy
8.5.10. Physical Security Policy
8.5.11. Privacy and Confidentiality Policy
8.5.12. Remote Access Policy
8.5.13. Security Lifecycle and Audit Policy
8.5.14. Smartphone-PDA Policy
8.5.15. Third Party IT Service Organizations Policy

8.5.16. Virus Protection Policy
8.5.17. Wireless Communication Policy

9. ENFORCEMENT

Any User of County Computing Assets, found to have violated this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

10. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	June 1, 2007	3.1.4 and 8.5 3.6.1.1.1.1 and 4.4 3.6.1.3.2	Add a reference to the full listing of policies Changes that reflect "Matter" as the defining noun Add "or discrimination"
1.2	May 5, 2006	3.6.1.1.1	Added language prohibiting viewing, etc. obscene and illegal material
		9.0	Removed the word "purposely"
1.1	April 2, 2005	3.6.1.1.6	Added section: "Exporting, exploring, sharing or using for personal gain, data contained… This includes Users developing applications or accessing data for their own department or another County department."
1.1	April 2, 2005	4.2	Added "officers, agents"
1.0	April 2, 2004	All	New policy entitled *ISP Acceptable Use Policy*

ATTACHMENT

COUNTY OF SAN LUIS OBISPO

Countywide Information Security Program

Computer Information Security Acceptable Use Policy Acknowledgement

I acknowledge receipt of this policy and understand that I am bound by its contents:

SIGNATURE	
NAME	
TITLE	
DEPARTMENT	
DATE	